PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-186825

(43)Date of publication of application : 02.07.2004

(51)Int.Cl. H04L 9/08
G06F 12/14
G11B 20/10
G11B 20/12
H04L 9/14

(21)Application number : 2002-348925

(22)Date of filing : 29.11.2002

(71)Applicant : TOSHIBA CORP

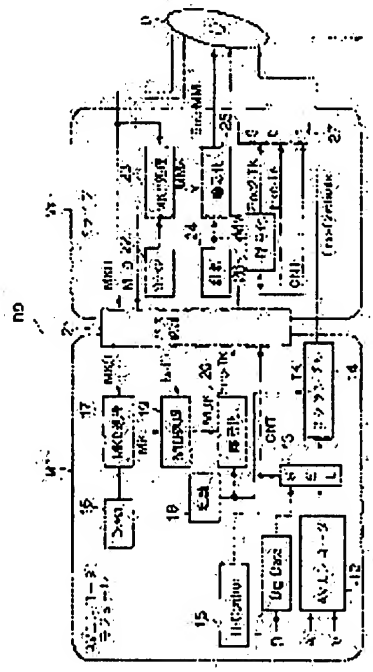
(72)Inventor : KOJIMA TADASHI
YAMADA HISASHI
KATO HIROSHI
ISHIHARA ATSUSHI
TAIRA KAZUHIKO

(54) CONTENTS CONTROL METHOD, RECORDING REPRODUCER, AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a contents control method which allows contents to be shifted while avoiding diffusing the contents and guarantee a certain reproduction compatibility in the conventional general-purpose apparatus.

SOLUTION: The contents control method comprises a step of enciphering contents data using a first key (TK) enciphering the first key using a plurality of kinds of second keys (MUK); multiply enciphering the enciphered first key (Enc-TK) using a third key (MM); enciphering the third key using a fourth key (MMK), recording on a recording medium the enciphered contents data (Enc-Contents), the first key (Enc-TK) of a medium key enciphered by the second keys; and the first key (Enc2-TK) of a shift key, multiply enciphered by the second and the third keys, and recording the third key (Enc-MM) enciphered by the fourth key on a secrete area, thus controlling the



contents by the shift key and the medium key.

LEGAL STATUS

[Date of request for examination]	29.11.2002
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3878542
[Date of registration]	10.11.2006
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]
This invention relates to the record regenerative apparatus using the contents management method and this which manage contents data, the contents management method which enables fixed migration of contents data while preventing an unrestricted illegal copy especially about the record medium with which contents data etc. were recorded by this and a record regenerative apparatus, and the record medium of this.
[0002]
[Description of the Prior Art]
With the record medium of voice or an image, there are a compact disk and a laser disk as a medium which records the digitized information (for example, a document, voice, an image, a program, etc.) conventionally. Moreover, there are a floppy disk and a hard disk in the program of a computer etc., or the record medium of data. Moreover, in addition to these record media, DVD (Digital Versatile Disk) which is a mass record medium is developed.
[0003]
in such various digital storage media, since the digital data (compression, coding, etc. are carried out and it can decode -- it contains) is recorded as it is when recording, copying the recorded data to other media can be copied having no loss of tone quality or image quality, and easily. Therefore, by these digital storage media, a duplicate is made in large quantities, things are made, and there are problems, such as infringement of copyright.
[0004]
According to this, the copyright protection system called CSS (Content Scramble System) about the DVD-video disk only for playbacks is introduced by making illegal copy prevention of contents into a technical problem as the contents encryption / decryption approach of the conventional technique (for example, patent reference 1 reference).
[0005]
[Patent reference 1]
JP,09-136709,A.
[0006]
[Problem(s) to be Solved by the Invention]
However, conventionally [above-mentioned], with equipment, while performing contents migration, preventing and carrying out the protection of copyrights of the illegal copy, it cannot be told to coincidence that contents are reproduced with the conventional regenerative apparatus which is a general aviation. That is, there is a problem that the convenience of the user of also performing playback by equipment conventionally moreover is not securable, moving contents data suitably.
[0007]
While this invention enables migration of contents, preventing diffusion of contents, it aims at offering

the contents management method, record regenerative apparatus, and record medium which also guarantee the minimum playback compatibility in conventional general-purpose equipment.
[0008]
[Means for Solving the Problem]
Contents data are enciphered with the 1st key (TK) so that this invention may solve the above-mentioned technical problem. Said 1st key is enciphered with two or more kinds of 2nd key (MUK) which was able to be defined beforehand. Multiplex encryption of said 1st enciphered key (Enc-TK) is carried out with the 3rd key (MM). The contents data which enciphered with the 4th key (MMK) which was able to define said 3rd key beforehand, and were enciphered with said 1st key (Enc-Contents), The 1st key enciphered with said two or more kinds of 2nd key defined beforehand (Enc-TK), The 1st key (Enc2-TK) by which multiplex encryption was carried out with the 3rd key (MM) in said 1st enciphered key (Enc-TK) is recorded on a record medium. It is the contents management method characterized by what the 3rd key (Enc-MM) enciphered with said 4th key is recorded for on the secrecy field of said record medium.
[0009]
As described above, this invention is a navigation key (Move-Key) which is a cryptographic key for contents migration control, is recording the 1st key (Enc2-TK) which is a title key which carried out multiplex encryption of the cryptographic key of contents with the 2nd-3rd key and by which multiplex encryption was carried out on a record medium, and enables contents migration in fixed constraint. The medium key (Enc-TK) which enciphered the title key (TK) with the 2nd key (MKB, M-ID) only at once and which is the title key by which the media binding head was carried out is also recorded on a different field in order to make contents refreshable on the other hand also with the not a special-purpose machine but conventional general aviation corresponding to a navigation key (Move-Key). Thereby, while enabling playback with a general aviation by the medium key (Enc-TK), contents migration is enabled by the navigation key (Move-Key), preventing diffusion of contents data.
When recording contents data on the 1st record medium (D1) from the source of contents data (S) where the contents data to which migration was permitted were further stored between record media, this invention The contents data enciphered with the 1st key (TK) (Enc-Contents), The 1st key enciphered with the 2nd key which is a contents cryptographic key (MB-KEY) bound to the record medium (Enc-TK), The cryptographic key for contents migration control by which multiplex encryption was carried out with the 2nd-3rd key (Enc2-TK), When recording on the record medium (D1) of **** 1 (flow 1) and moving contents data to the 2nd record medium (D2) from said 1st record medium (D1) While after [decode] re-enciphering said contents data and recording only encryption contents data and said cryptographic key for contents migration control on the 2nd record medium It is the contents management method characterized by what (flow 2) the cryptographic key for contents migration control currently recorded on said 1st record medium is eliminated for.
[0010]
Two keys and the medium key for general aviation playback (Enc-TK) to which the contents management method concerning this invention is specified, and mentioned the moving method of contents above, About the navigation key (Move-Key) for contents migration, it sets to record of the contents data from the source of contents data (S) to the 1st disk (D1). While recording two keys and enabling migration of future contents, coincidence is made to correspond also to playback by general aviations other than a special-purpose machine. On the occasion of the migration of contents data on the 2nd disk (D2) from the 1st disk (D1), a navigation key (Move-Key) is deleted from the 1st disk (D1), and it leaves only the medium key (Enc-TK) for general aviation playback. Thereby, it becomes impossible to perform subsequent migration and playback of a general aviation can be performed further in the future. In migration of contents data on the 2nd disk, since only a navigation key (Move-Key) is recorded, it becomes reproducible only with a special-purpose machine, and the migration to the disk of the 3rd henceforth etc. can be continued further in the future.
[0011]
Though playback and migration of contents data are enabled and diffusion of contents data is prevented

with the record approach to the first disk and the subsequent moving method which were mentioned above, the contents management method concerning this invention enables migration of contents data, and offers a contents management method reproducible also not only in a special-purpose machine but the conventional general aviation, a record regenerative apparatus, and a record medium further.
[0012]
[Embodiment of the Invention]
Hereafter, with reference to a drawing, the contents management method concerning this invention, a record regenerative apparatus, and a record medium are explained to a detail. An example of the record medium with which the block diagram showing an example of the decode by the general approach of contents that the block diagram, drawing 2 , and drawing 3 which show an example of encryption by the contents management method which drawing 1 requires for this invention were enciphered, and drawing 4 recorded the enciphered contents, and drawing 5 are the explanatory views showing an example of migration of the navigation key (Move-Key:Enc2-TK) by the contents management method concerning this invention, and a medium key (MB-Key:Enc-TK).
[0013]
<The outline of the contents management method concerning this invention>
The encryption approach and its decode approach are explained below as an outline of the contents management method concerning this invention using introduction and a drawing. the navigation key (Move-Key:Enc2-TK) which guarantees migration of contents data in the contents management method concerning this invention, and the medium key (MB-Key:Enc-TK) which guarantees also reproducing the regenerative apparatus by the conventional general aviations (for example, optical disk unit etc.) -- encryption contents data -- a record medium -- ** -- it is characterized by what is recorded.
(Encryption)
In drawing 1 , work of AV encoder module M1 and work of drive V1 can explain the contents data encryption and the record approach in the contents management method concerning this invention. In AV encoder module M1 of drawing 1 , after an image (V) voice (A) signal is encoded by DVD format with the AV encoder 12 and is chosen by the selector 13 with digital data 11, scramble (encryption) processing is carried out with a title key (TK) in the scramble circuit 14, and it is recorded on Disk D as (Enc-Contents).
[0014]
The title key at this time (TK) is generated by the random number generator 18. It is enciphered by the cryptographic key (MUK) in the encryption circuit 20, and the encryption key TK turns into an encryption title key (Enc-TK). Here, the cryptographic key (MUK) which enciphered the title key (TK) is obtained by carrying out MKB processing of the device key K1 (DvK116) by the MKB processing 17 with the data (MKB) read from the archive medium, generating a media key (MMK), carrying out MID processing and generating this by the MID processing 19, using the media proper information (M-ID) further read from the archive medium.
Furthermore, multiplex encryption of the enciphered title key (Enc-TK) is carried out with a secrecy key (MM), a multiplex encryption title key (Enc2-TK) is generated, and a selector 27 is supplied like an encryption title key (Enc-TK).
[0015]
Here, a secrecy key (MM) is supplied by the random number generator 24. MKB to which the device key (DvK2) of drive V1 proper was given from the record medium performs MKB processing by the MKB processing 23, this secrecy key (MM) is enciphered by the obtained cryptographic key (MMK), and an encryption cryptographic key (Enc-MM) is obtained.
Thus, the obtained contents data (Enc-Contents) which were enciphered, the title key (Enc-TK) (= medium key (MB-Key)) enciphered by the cryptographic key (MUK), and the title key (Enc2-TK) (= navigation key (Move-Key)) by which multiplex encryption was carried out with the 2nd-3rd key are recorded on the storage region of optical disk D, respectively. Furthermore, the 3rd key (Enc-MM) with which the point was enciphered is recorded on the secrecy field of optical disk D. An example of record to optical disk D of these signals is shown in drawing 4 .

[0016]
namely, the selector 27 according to the control signal from R-Control15 both whose navigation keys (Move-Key;Enc2-TK) and medium keys (MB-Key;Enc-TK) (after contents migration, on the other hand) which are the description of the contents management method concerning this invention here are record processing control sections -- minding -- optical disk D -- ** -- it is recorded.
[0017]
Here, it has prevented the same key information (MK) being generated by two or more device keys (Dvk), and copying the information recorded on the optical disk archive medium to other media the whole round head by a media binding head being further performed using media proper information (M-ID), in order to realize transposition with playback in other regenerative apparatus.
[0018]
Moreover, two cryptographic keys, the navigation key (Move-Key;Enc2-TK), and the medium key (MB-Key;Enc-TK) enable playback with the general aviation under fixed conditions, and migration processing of restrictive contents data by being alternatively recorded on optical disk D in the case of the copy of contents, or migration so that it may explain in full detail behind.
[0019]
(The two playback approaches)
Thus, as optical disk D on which the key information enciphered as the contents data enciphered as drawing 4 showed was recorded is shown below, optical disk D on which the medium key (MB-Key;Enc-TK) was recorded at least is reproducible with the conventional general-purpose optical disk regenerative apparatus. Furthermore, optical disk D on which only the navigation key (Move-Key;Enc2-TK) was recorded is reproduced only with the optical disk regenerative apparatus with which the contents management method concerning this invention is performed.
[0020]
That is, drawing 2 is drawing showing the decode processing performed only using the medium key (MB-Key;Enc-TK) concerning this invention with the regenerative apparatus which is the conventional general aviation. In this drawing, the media key block information (MKB) and media proper information (M-ID) that optical disk D on which the medium key (MB-Key;Enc-TK) was recorded at least is beforehand recorded on media through the drive V2, and a medium key (MB-Key;Enc-TK) are supplied to AV decoder module M2 through the bus authentication 21. Furthermore, the enciphered contents data (Enc-Contents) are supplied to AV decoder module M2.
[0021]
Descrambling (decryption) processing is carried out with a title key (TK) by descrambling 29, and this encryption contents data (Enc-Contents) is supplied to the AV decoder 30, and is reproduced. Here, an encryption title key (Enc-TK) is read from Disk D, is sent to the decode section 28, and a title key (TK) is obtained by decoding by the cryptographic key (MUK). Moreover, a cryptographic key (MUK) is acquired by the MKB processing 17 using media key block information (MKB) and media proper information (M-ID), and the MID processing 19 like a record side.
The contents data of optical disk D on which the medium key (MB-Key;Enc-TK) was recorded also with the conventional optical disk regenerative apparatus which do not perform processing by the contents data control approach concerning this invention by this become possible [reproducing].
On the other hand, as shown in drawing 3 , it is reproducible for the first time by performing processing by the contents data control approach concerning this invention in optical disk D to which only the navigation key (Move-Key;Enc2-TK) is given.
Namely, the drive V1 to which media key block information (MKB), an encryption title key (Enc-MM), a multiplex encryption title key (Enc2-TK), and encryption contents (Enc-Contents) were given from the optical disk unit With the key (MMK) obtained by taking MKB processing 23 with the device key (DvK2) of drive V1 proper, it decodes by the decode section 31 and a secrecy key (MM) is obtained. By this The title key (Enc2-TK) by which multiplex encryption was carried out is decoded to an encryption title key (Enc-TK), and a module M2 is supplied through the bus authentication 21.
[0022]

By the module M2, by the cryptographic key (MUK) which carried out the device key (DvK) of module M2 proper MKB processing 17 using media key block information (MKB), carried out MID processing 19 using media proper information (M-ID), and was obtained, an encryption title key (Enc-TK) is decoded in the decode section 28, and a title key (TK) is obtained.
[0023]
By using this title key (TK), contents data can be supplied to the AV decoder 30 by decoding the enciphered contents data (Enc-Contents) in the descrambling section 29.
Thus, in optical disk D which gave only the navigation key (Move-Key;Enc2-TK), it becomes movable [which it is later reproduced and mentioned only with the optical disk record regenerative apparatus which performs processing by the contents data control approach concerning this invention].
(Contents migration by the contents data control approach concerning this invention)
Next, the outline is explained about an example of the moving method of the contents data based on the contents data control approach concerning this invention. In drawing 5 , a limit can be given about playback, or a copy and migration by making this record on a record medium suitably by the contents data control approach concerning this invention using two kinds of keys of a navigation key (Move-Key:, i.e., Enc2-TK) and a medium key (MB-Key:, i.e., Enc-TK). Namely, as for archive media, such as an optical disk, according to the contents data control approach concerning this invention, three kinds of only "a medium key (MB-Key) and a navigation key (Move-Key)", "a medium key (MB-Key)", and "a navigation key (Move-Key)" exist. Here, explanation is omitted about contents data and outline explanation is given only about these two medium keys and navigation keys.
In drawing 5 , as for the source contents S by which the copy limit was carried out, a medium key (MB-Key) + navigation key (Move-Key) is first given to the first disk D1 (record medium). Thereby, playback also of a common regenerative apparatus or the regenerative apparatus concerning this invention is attained.
Next, when moving the contents data in a disk D1 to the new disk D2 with the regenerative apparatus concerning this invention, a disk D1 becomes disk D1' which is deleted in a navigation key (Move-Key) and has only a medium key (MB-Key). Only a navigation key (Move-Key) is recorded on the new disk D2. Thereby, disk D1' becomes possible [only reproducing with a common regenerative apparatus]. Moreover, a disk D2 is unreproducible with a common regenerative apparatus, it can reproduce only with the record regenerative apparatus concerning this invention, or migration processing can be performed.
Furthermore, when moving the contents data of the disk D2 used as such a navigation key (Move-Key) to the new optical disk D3, the navigation key (Move-Key) of an optical disk D2 is deleted by the regenerative apparatus concerning this invention, and serves as playback impossible with it. Only a navigation key (Move-Key) is recorded, it can reproduce only with the record regenerative apparatus concerning this invention, or an optical disk D3 can perform migration processing.
Moreover, further, migration of the contents data of optical disk D by the record regenerative apparatus concerning this invention does not restrict the object only to an optical disk, and is aimed at common digital storage media, such as SD (Secure Digital) card. The navigation key (Move-Key) from the optical disk D3 to the SD (Secure Digital) card D4 is movable here. Like the case of migration of an optical disk D2 to the previous optical disk D3, an optical disk D3 A navigation key (Move-Key) is deleted, reproducing becomes impossible, the SD (Secure Digital) card D4 can be reproduced only with the record regenerative apparatus which only a navigation key (Move-Key) is recorded and is applied to this invention, or migration processing can be performed.
<The example of application of the contents management method concerning this invention>
Next, the contents management method concerning this invention is explained to a detail using a drawing about the operation gestalt at the time of applying to a concrete optical disk record regenerative apparatus. The block diagram explaining an example of the detail of the encryption approach at the time of applying the block diagram and drawing 7 which show an example of the structure of the record regenerative apparatus which applied the contents management method which drawing 6 requires for this invention to a record regenerative apparatus, and drawing 8 are the block diagrams explaining an

example of the detail of the decode approach.
[0024]
(Record regenerative apparatus)
The optical disk record regenerative apparatus A with which the contents management method concerning this invention is applied is raised to drawing 6 , and the optical disk record regenerative apparatus A has a control section by the system control section 162 which manages the whole actuation, RAM161 and ROM160 used as activity area, and the servo control section 152. Furthermore, the detecting signal for the optical pickup 154 which irradiates a laser beam, and the playback from here is received in optical disk D, and the signal for record is supplied, and it has the signal-processing section 156 which performs ECC processing etc., has the bus authentication section 21 mentioned above to drawing 1 etc., and has further the data-processing section 158 which has the bus authentication section 21 similarly through a cable, and performs encoding decoding etc. Moreover, the media reader writer 166 which is the interface of record media, such as SD card, is connected to the signal-processing section 156. Moreover, RAM159 and the interface 165 which output and input a signal with an external device are connected to the data-processing section 158.
Moreover, it has servo control system each processing circuit 155 connected to the further above-mentioned servo control section 152, the actuator driver 153 connected to this, and the disk motor 151.
[0025]
In optical disk unit A which has such a configuration, the system control section 162 uses RAM161 as activity area, and performs predetermined actuation according to the program containing this invention recorded on ROM160. The laser beam outputted from the optical pickup 154 is irradiated by optical disk D. The reflected light from optical disk D is changed into an electrical signal with a head amplifier. This electrical signal is inputted into the signal-processing section 156. An RF amplifier etc. is contained in the signal-processing section 156.
[0026]
At the time of record actuation, encryption processing explained in full detail using drawing 1 is performed to contents data, and record processing is made by optical disk D. Furthermore, if it states in detail, the write-in clock made in the light channel circuit which the data-processing section 158 does not illustrate will be used. Error detecting code (EDC) and ID are added to the contents data sent through an interface 165. Data scramble processing by the encryption mentioned above is performed, and an error correcting code (ECC) is added further, and a synchronizing signal is added and combined, it becomes irregular except a synchronizing signal, and a signal is recorded on optical disk D by the laser beam controlled by the optimal light strategy for correspondence media.
[0027]
At the time of playback actuation, decode processing explained in full detail using drawing 2 and drawing 3 is performed to contents data, and regeneration of the contents data stored in optical disk D is performed. Furthermore, if it states in detail, the RF signal read from the head amplifier of an optical pickup 154 will let the optimal equalizer pass, and will be sent to the PLL circuit which is not illustrated in the signal-processing section 156. Channel data are read with the read-out clock made in the PLL circuit. Decode processing by the decode mentioned above is performed, the read data are further synchronized in the data-processing section 158, and symbol data are read. Descrambling processing by the error correction or the decode processing mentioned above is performed after that, and it is transmitted outside through an interface 165.
[0028]
Thus, record processing and regeneration are given with the optical disk record regenerative apparatus A mentioned above.
[0029]
Moreover, the signal-processing section 156 and the data-processing section 158 have the bus authentication section 21, respectively, remove the connector of the cable to which both are connected, extract a signal, and are performing the cure to the third person who is going to copy illegally. That is, each bus authentication section 21 has the random number generator which is not illustrated,

respectively, generated the same cryptographic key by this, and after enciphering transmit information, it has transmitted to the other party. By the device of the other party which received transmit information, the transmit information enciphered by the same cryptographic key generated by itself is decoded. Contents data etc. can be copied illegally, even if it removes the connector of a cable and extracts a signal, unless it is very difficult for a third person to reproduce this and the cryptographic key at that time can be reproduced, since this cryptographic key changes and is generated according to predetermined time.

[0030]

(Secrecy of the cryptographic key by modulation / recovery processing)

Here, secrecy processing of cryptographic key information in which the actuation of a modulation and a demodulator circuit currently performed by the digital disposal circuit 156 was applied is described below. In addition, in the important section of the contents management method for the record processing which drawing 7 shows, since AV encoder module M1 is equivalent to AV encoder module M1 shown in drawing 1 and AV decoder module M2 is equivalent to AV decoder module M2 shown in drawing 3 in the important section of the contents management method for the record processing which drawing 8 shows, explanation is omitted here.

[0031]

In addition to the configuration of the drive section V1 of drawing 1 , the ECC circuit etc. is shown in the drive section V3 of drawing 7 . That is, an error correcting code is added by the ECC circuit 43, and the signal from the contents scramble 14 which is the Maine data is modulated in a modulation circuit 44. Furthermore, after error-correcting-code-izing by the ECC circuit 47, the 2nd modulation circuit's 48 becoming irregular and a selector's 45 also permuting the enciphered secrecy key (Enc-MM) with some Maine data, it is recorded on the storage region of optical disk D by the light channel circuit 46.

On the other hand in the drive section V4 of drawing 8 , the data with which the error correcting code was added can be read from optical disk D, it can get over in the 2nd demodulator circuit 45, and the ECC circuit 46 can extract an encryption secrecy key (Enc-MM). On the other hand, since an encryption secrecy key (Enc-MM) is modulated and it is recorded in drawing 7 using the 2nd modulator 48 which is different in the modulator 44 of the Maine data, in the demodulator 42 of the Maine data of the read-out section, it cannot restore to an encryption secrecy key (Enc-MM), but is processed as error data. Thereby, a third person cannot extract an encryption secrecy key (Enc-MM) for the purpose of an illegal copy. Thus, by applying modulation / recovery processing, by the usual Maine data recovery processing, undetectable secrecy information can be made and processing equivalent to having recorded encryption key information (Enc-MM) on the secrecy field substantially, and having reproduced can be performed. Thereby, even if it is a passive record medium like an optical disk, it becomes possible to build an advanced protection system.

[0032]

(Migration flow chart 1)

Next, the migration processing between the record media of the contents data explained briefly previously is explained to a detail using a flow chart. The flow chart and drawing 10 which show the actuation which records the contents enciphered by the contents management method which drawing 9 requires for this invention, and key information on a record medium D1 The flow chart and drawing 11 which show the actuation in the case of moving contents to other record media D2 from a record medium D1 The flow chart and drawing 12 which show the actuation in the case of moving contents to other record media D3 from a record medium D2 are a flow chart which shows the actuation in the case of performing this migration with a channel down.

[0033]

The contents management method concerning this invention is realized by the configuration of the signal-processing section 156 in an optical disk record regenerative apparatus, or the data-processing section 158 as mentioned above, but these processings are possible even if the program which described the procedure of giving a contents management method to detection information realizes. Hereafter, the contents management method concerning this invention is explained to a detail using a flow chart.

[0034]
In the flow chart which drawing 9 shows, the case where contents data are copied to the record media D1, such as optical disk D, is explained from the contents data S by which the copy limit was carried out.
The media key block information (MKB) and media proper information (M-ID) for generating key information (MK) are read from introduction and a record medium D1, and these are transmitted to AV encoder section M1 (S11). And the decode key (DvK1) 16 of a device proper extracts key information (MK) from media key block information (MKB) in AV encoder section M1. And the cryptographic key (MUK) for title key codes is generated from key information (MK) and media proper information (M-ID) (S12).
[0035]
Next, random-number-generation processing generates a title key (TK). And scramble encryption of the contents data with which protection of copyrights was specified is carried out with a title key (TK) (S13). Next, a title key (TK) is enciphered with the key (MUK) for title key codes, and the enciphered title key (Enc-TK) is generated (S13). Next, encryption contents (Enc-Contents) and an encryption title key (Enc-TK) are transmitted to drive V1 through bus authentication processing (S14).
[0036]
Here, it judges whether migration authorization of the record contents is carried out (S15). If the permission is granted, random-number-generation processing will generate a secrecy key (MM). And multiplex encryption of the encryption title key (Enc-TK) is carried out with a secrecy key (MM), and a multiplex encryption title key (Enc2-TK) is generated. And the medium key (MB-Key) of encryption contents (Enc-Contents) and an encryption title key (Enc-TK) group and the navigation key (Move-Key) of a multiplex encryption title key (Enc2-TK) group are recorded on a record medium D1 to a record medium D1 (S16).
[0037]
Furthermore, the device key in drive V1 (DvK2) detects a cryptographic key (MMK) from media key block information (MKB). A secrecy key (MM) is enciphered by the cryptographic key (MMK), and an encryption cryptographic key (Enc-MM) is generated (S17). And an encryption cryptographic key (Enc-MM) signal is recorded on a secrecy field (S18).
[0038]
Moreover, if a permission is not granted at step S15, the medium key (MB-Key) of encryption contents (Enc-Contents) and an encryption title key (Enc-TK) group is recorded on a record medium D1 (S19).
[0039]
Contents data are enciphered by these processings and both the navigation keys (Move-Key;Enc2-TK) and medium keys (MB-Key;Enc-TK) (or only medium key) which are the description of the contents management method concerning this invention are recorded on an optical disk D1.
[0040]
(Migration flow chart 2)
In the flow chart which drawing 10 shows, the actuation in the case of moving contents to other record media D2 is explained from a record medium D1.
First, a cryptographic key (MUK2) is generated for the migration place record medium D2 to media key block information (MKB), and media proper information (M-ID) from read-out and these (S21). Next, a record medium D1 is set and contents management information is detected (S22). Here, it judges whether there are any medium key (MB-Key) and navigation key (Move-Key) of correspondence contents (S23).
[0041]
At step S23, if it is judged that there is only a navigation key (Move-Key), media key block information (MKB) and a device key (DvK2) detect a cryptographic key (MMK), a secrecy key (MM) will be detected, a multiplex encryption title key (Enc2-TK2) will be decoded [an encryption cryptographic key (Enc-MM) will be decoded,] with a secrecy key (MM), and an encryption title key (Enc-TK) will be generated (S31).

[0042]
If there are both a medium key (MB-Key) and a navigation key (Move-Key) at step S23, through bus authentication, the media key block information (MKB) and media proper information (M-ID) on a record medium D1 will be transmitted, and the decode key (DvK1) of a device proper will detect a cryptographic key (MUK) (S24). Furthermore, an encryption title key (Enc-TK) is decoded by the cryptographic key (MUK), and a title key (TK) is generated. Furthermore, with the title key (TK2) which decoded encryption contents with read-out and a title key (TK) from the record medium D1, and was generated with a new random number generator, a re-scramble (encryption) is carried out and it records temporarily (S25). And the multiplex encryption title key (Enc2-TK) which is the navigation key (Move-Key) of the correspondence contents of a record medium D1 is eliminated (S26).
[0043]
Next, a record medium is changed into a record medium D2, a title key (TK2) is enciphered by the cryptographic key (MUK2), and an encryption title key (Enc-TK2) is generated (S27). And the new secrecy key in a record drive (MM2) is generated, multiplex encryption of the encryption title key (Enc-TK2) is carried out, and a multiplex encryption title key (Enc2-TK2) is generated.
[0044]
And the media key block information (MKB) and the device key (DvK2) of a record medium D2 generate a cryptographic key (MMK), a secrecy key (MM2) is enciphered and an encryption cryptographic key (Enc-MM2) is generated (S28). Next, the encryption contents (Enc-Contents) and the multiplex encryption title key (Enc2-TK2) which were enciphered with the title key (TK2) are recorded on a record medium D2. Furthermore, an encryption cryptographic key (Enc-MM2) is recorded on a secrecy field (S29).
[0045]
Moreover, if it becomes having no navigation key (Move-Key) at step S23, it will consider as migration disapproval (S30).
[0046]
Thereby, although the record medium D1 of a moved material is deleted, and serves as only a medium key (MB-Key), and it becomes impossible for contents data to move it and it can reproduce a navigation key (Move-Key) with the regenerative apparatus which is the conventional general aviation, it will be in a condition [that it cannot move]. On the other hand, the record medium D2 of a migration place serves as only a navigation key (Move-Key), and will be in the condition in which playback and migration beyond it are possible only with the special-purpose machine in which the contents management method concerning this invention is possible.
(Migration flow chart 3)
In the flow chart which drawing 11 shows, the actuation in the case of moving contents to other record media D3 is explained from a record medium D2.
From introduction and the migration place record medium D3, media key block information (MKB) and media proper information (M-ID) are read, and a cryptographic key (MUK2) is generated (S21). Next, a record medium D2 is set and contents management information is detected (S22). And it is judged whether there are any medium key (MB-Key) and navigation key (Move-Key) of correspondence contents (S23).
[0047]
If a navigation key (Move-Key) becomes nothing, contents data will serve as migration disapproval (S30).
[0048]
If it is judged that there is only a navigation key (Move-Key), media key block information (MKB) and a device key (DvK2) will extract a cryptographic key (MMK). And an encryption cryptographic key (Enc-MM) is decoded, a secrecy key (MM) is detected, a multiplex encryption title key (Enc2-TK2) is decoded with a secrecy key (MM), and an encryption title key (Enc-TK2) is generated (S31).
[0049]
If it is judged at step S23 that there are a medium key (MB-Key) and a navigation key (Move-Key),

through bus authentication, the media key block information (MKB) and media proper information (M-ID) on a record medium D2 will be transmitted, and the cryptographic key (MUK2) of a title key will be detected by the decode key (DvK1) of a device proper (S42). Next, an encryption title key (Enc-TK) is decoded by the cryptographic key (MUK2) of a title key, and a title key (TK2) is detected. and a record medium D2 to encryption contents (Enc-Contents) -- read-out -- it stores temporarily (S43). And the multiplex encryption title key (Enc2-TK2) which is the navigation key (Move-Key) of the correspondence contents of a record medium D2 is eliminated (S26).

[0050]

Next, a record medium is changed into a record medium D3, a title key (TK2) is enciphered by the cryptographic key (MUK2), and an encryption title key (Enc-TK3) is generated (S27). Next, the new secrecy key in a record drive (MM3) is generated, multiplex encryption of the encryption title key (Enc-TK3) is carried out, and a multiplex encryption title key (Enc2-TK3) is generated. And the media key block information (MKB) and the device key (DvK2) of a record medium D3 generate a cryptographic key (MMK), a secrecy key (MM3) is enciphered and an encryption cryptographic key (Enc-MM3) is generated (S28). And the encryption contents (Enc-Contents) and the multiplex encryption title key (Enc2-TK3) which were enciphered with the title key (TK2) are recorded on a record medium D3, and an encryption cryptographic key (Enc-MM3) is recorded on the secrecy field (S29). In addition, although the encryption title key (Enc-TK3) in the flow chart 3 of drawing 11 includes many processes which are common in the flow chart 2 of drawing 10 , in steps S42 and S43, it differs in that encipher a title key (TK2) by the cryptographic key (MUK2), and the encryption title key (Enc-TK3) is generated.

[0051]

Thereby, the record medium D2 of a moved material is deleted in a navigation key (Move-Key), and becomes migration of contents data and unreproducible. On the other hand, the record medium D3 of a migration place serves as only a navigation key (Move-Key), and will be in the condition in which playback and migration beyond it are possible only with the special-purpose machine in which the contents management method concerning this invention is possible.

Moreover, the target record medium [management method / concerning this invention / contents] can be aimed at the common digital storage medium of SD (Secure Digital) card D4 grade as shown not only in an optical disk but in drawing 5 .

[0052]

(Migration flow chart 4)

Furthermore, in migration processing of the contents data shown with the flow chart of drawing 11 , the case where carry out a channel down and the audio source data (5.1 Channel) of multi-channel are processed to two channels is explained. Although these processings are equivalent to the processing fundamentally shown with the flow chart of drawing 11 , they are performed by the processing which step S42 and step S43 of a flow chart of drawing 11 place with step S44, and replace.

That is, in step S44 of the flow chart of drawing 12 , the enciphered title key (Enc-TK) is decoded by the cryptographic key (MUK2), and a title key (TK2) is generated. And encryption contents (Enc-Contents) are read from a record medium D2, and it decodes with a title key (TK2). Furthermore, the channel down of the audio source data of multi-channel is carried out at two channels, and it scrambles again with the title key (TK3) generated with the random number generator (encryption), and records temporarily (S44).

[0053]

In such processing, carrying out the channel down of the audio source data (5.1 Channel) at two channels, contents data can be moved to the new record medium D3 from a record medium D2, and the operation effectiveness is equivalent to migration processing of the flow chart of drawing 11 .

[0054]

(The key information for every music file, and the growth approach of a key)

Moreover, the target contents [management method / concerning this invention / contents] data can still take the gestalt of two or more voice files as music information on two or more music. Although for example, an image file and an image file are sufficient as two or more information, hereafter, an

example is taken to a voice file and it explains to it. In this gestalt, what is different one by one for every multi-file of this is prepared, it is enciphering, respectively and the title key (TK) which the random number generator 18 shown in drawing 1 supplies becomes movable to other record media in every music of music information. Thereby, the degree of freedom of contents use of a user can be raised very much.
However, if two or more title keys (TK) are made to correspond one by one and a navigation key (Move-Key=Enc2-TK) is generated, the need that only the number of two or more music files prepares the secrecy key (MM) in the drive section V1 will come out. However, if only the number of music prepares a secrecy key (MM) and this is all stored in the secrecy field of optical disk D, a secrecy field is not desirable from big storage capacity being needed and causing increase of storage capacity. By the secrecy information recording method using modulation / recovery processing especially mentioned above, some Maine data will be destroyed, secrecy information will be recorded, and since it is not desirable to regeneration of the Maine data, reduction of secrecy information is desirable as much as possible.
[0055]
Then, two or more keys in a fixed procedure are proliferated for a secrecy key (MM) to origin, this is used for encryption, considering as the secrecy key (MM) which became the origin of growth stores in a secrecy field, and it becomes possible to manage multiple files, respectively, reducing the storage capacity of a secrecy field.
Drawing 13 is drawing showing the generation method of the secrecy key (MM) in the contents management method concerning this invention, and is set to this drawing. In the random number generator 24 grade of drawing 1 , the secrecy key (MM1) based on the key former data (MM) generated from a random number G61 is generated. After that The identification code of contents data, Or a new secrecy key (MM2-MMn) is generated by carrying out the multiplication of the specific function K by the count decided by a rank number etc. The title key (Enc-TK1 - Enc-TKn) 63-1 with which plurality was enciphered - n are carried out encryption 64 using two or more of these secrecy keys (MM2-MMn), respectively.
[0056]
however -- the encryption cryptographic key (Enc-MM) as which storing in a secrecy field enciphered key former data (MM) -- since -- since the memory capacity of a required secrecy field does not increase, it becomes possible [performing contents management with high security about many multi-files].
(Management information)
In the contents management method concerning this invention, since playback and migration of contents data are managed by the navigation key (Move-Key) and the medium key (MB-Key), these cryptographic key files are data important for encryption contents and an EQC. That is, unless it can decode an encryption cryptographic key, encryption contents can also perform neither decode nor playback. Then, as shown in drawing 14 , the navigation key (Move-Key) file and the medium key (MB-Key) file are prepared in a file space different, respectively at the data area of a record medium (for example, optical disk). And the dependability of data is raised by arranging one table to each ECC block, and carrying out 4-fold writing to 4ECC block respectively.
[0057]
Moreover, the table of these files is shown in drawing 15 . That is, three kinds of only "a medium key (MB-Key) and a navigation key (Move-Key)", "a medium key (MB-Key)", and "a navigation key (Move-Key)" exist in an archive medium. Moreover, when there are many contents files, it is required to be able to read easily the relation between a medium key (MB-Key) and a navigation key (Move-Key) from individual management to each contents cryptographic key. So, the table consists of the tables of a navigation key (Move-Key) and the tables of a medium key (MB-Key) which are shown in drawing 15 considering the existence information on the cryptographic key of the relation to each encryption cryptographic key, and the information used when the generation method of the secrecy key (MM) shown by drawing 13 was taken as an informational group. It becomes possible to judge easily whether

contents migration is possible about each contents data by looking through this table.
It is possible to apply to various operation gestalten according to various operation gestalten indicated above, even if it is easy to think of a modification with these still more various operation gestalten and it does not have invention-capacity by this contractor although this contractor can realize this invention. Therefore, this invention reaches the extensive range which is not contradictory to the indicated principle with the new description, and is not limited to the operation gestalt mentioned above.
[0058]
For example, in case the secrecy field where a secrecy key is stored uses modulation / recovery processing mentioned above, it may make the field of secrecy information record playback equivalent to record playback area where the Maine data are another. By taking such an approach, since it is lost that an error component can be added, spoiling the dependability of contents data of the Maine data is lost.
[0059]
[Effect of the Invention]
The navigation key which guarantees migration of contents data according to this invention as explained in full detail above (Move-Key:Enc2-TK), By recording the medium key (MB-Key:Enc-TK) which guarantees also reproducing the regenerative apparatus by the conventional general aviations (for example, optical disk unit etc.) on a record medium with encryption contents data In the record regenerative apparatus concerning this invention which can decode the secrecy key stored in the secrecy field, the playback and migration by the navigation key (Move-Key) are possible, and playback by the medium key (MB-Key) is guaranteed in the regenerative apparatus which is the conventional general aviation. Thereby, though diffusion of contents data is prevented, while the migration processing by the special-purpose machine is possible, it becomes possible to reproduce the contents data based on the conventional machine.
[Brief Description of the Drawings]
[Drawing 1] The block diagram showing an example of encryption by the contents management method concerning this invention.
[Drawing 2] The block diagram showing an example of the decode by the general approach of the contents enciphered by the contents management method concerning this invention.
[Drawing 3] The block diagram showing an example of the decode by the approach concerning this invention of the contents enciphered by the contents management method concerning this invention.
[Drawing 4] An example of the record medium which recorded the contents enciphered by the contents management method concerning this invention.
[Drawing 5] The explanatory view showing an example of migration of the navigation key (Move-Key:Enc2-TK) by the contents management method concerning this invention, and a medium key (MB-Key:Enc-TK).
[Drawing 6] The block diagram showing an example of the structure of the record regenerative apparatus which applied the contents management method concerning this invention.
[Drawing 7] The block diagram explaining an example of the detail of the encryption approach at the time of applying the contents management method concerning this invention to a record regenerative apparatus.
[Drawing 8] The block diagram explaining an example of the detail of the decode approach at the time of applying the contents management method concerning this invention to a record regenerative apparatus.
[Drawing 9] The flow chart which shows the actuation which records the contents enciphered by the contents management method concerning this invention, and key information on a record medium D1.
[Drawing 10] The flow chart which shows the actuation in the case of moving contents to other record media D2 from the record medium D1 with which the contents enciphered by the contents management method concerning this invention were recorded.
[Drawing 11] The flow chart which shows the actuation in the case of moving contents to other record media D3 from the record medium D2 with which the contents enciphered by the contents management method concerning this invention were recorded.

[Drawing 12] The flow chart which shows the actuation in the case of performing migration of contents to other record media [record medium / D2 / with which the contents enciphered by the contents management method concerning this invention were recorded] D3 with a channel down.
[Drawing 13] Drawing showing the generation method of the secrecy key (MM) in the contents management method concerning this invention.
[Drawing 14] Drawing showing an example of the storing field of the navigation key in the record medium in the contents management method concerning this invention (Move-Key:Enc2-TK), and a medium key (MB-Key:Enc-TK).
[Drawing 15] Drawing showing an example of the table of the navigation key in the record medium in the contents management method concerning this invention (Move-Key:Enc2-TK), and a medium key (MB-Key:Enc-TK).
[Description of Notations]
11 [-- MKB processing, 18 / -- A random number generator, 19 / -- MID processing, 20 / -- An encryption circuit, 21 / -- The bus authentication section, 22 / -- A device key, 23 / -- MKB processing, 24 / -- A random number generator, 25 / -- An encryption circuit, 26 / -- An encryption circuit, 27 / -- Selector.] -- Digital data, 15 -- R-Control (record control), 16 -- A device key, 17

[Translation done.]